AMENDMENTS TO THE CLAIMS

All pending claims and their present status are produced below.

1. (Currently Amended) A computer implemented method for gleaning file attributes independently of file format, the method comprising the steps of:

a non-application-specific file attribute manager receiving a plurality of files in a plurality of formats;

the file attribute manager scanning the plurality of received files in the plurality of formats;

the file attribute manager gleaning file attributes of a plurality of types from each of the plurality of scanned files in the plurality of formats, wherein the plurality of gleaned attribute types differ for protocols used to receive the plurality of scanned files and each of the plurality of scanned files are received according to one of the protocols;

the file attribute manager storing the file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database;

the file attribute manager indexing specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database;

examining one of the plurality of files;

retrieving from the plurality of records in the database a first record associated with the examined one of the plurality of files;

retrieving from the plurality of records in the database a second record associated with a malicious file;

analyzing the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record;

analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and

determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file.

2. (Cancelled)

3. (Previously Presented) The method of claim 1 wherein:

specific types of file attributes are gleaned from a specific file as a function of a format of the specific file.

4. (Previously Presented) The method of claim 1 wherein the file attribute manager indexing specific file attributes indexes according to a secure hash of the contents of each specific file.

5. (Previously Presented) The method of claim 1 wherein the file attribute manager indexing specific file attributes indexes according to a cyclical redundancy check of the contents of each specific file.

6. (Previously Presented) The method of claim 1 further comprising:

the file attribute manager receiving a plurality of copies of a selected file of the plurality of files; and

the file attribute manager storing each of the plurality of copies as a separate record in the plurality of records, each separate record indexed according to the contents of the selected file of the plurality of files, such that the each separate record can be accessed by a single index.

7. (Original) The method of claim 1 further comprising:

deleting records from the database after the records have been stored for a specific period of time.

8. (Previously Presented) The method of claim 1 wherein the non-application-specific file attribute manager is incorporated into one selected from the group consisting of:

a firewall;

an intrusion detection system;

an intrusion detection system application proxy;

a router;

a switch;

a standalone proxy;

a server;

a gateway;

an anti-virus detection system; and

a client.

9. (Currently Amended) A computer-readable storage medium containing a computer program product for gleaning file attributes independently of file format, the computer program product comprising program code for:

receiving a plurality of files in a plurality of formats;

scanning the plurality of received files in the plurality of formats;

gleaning file attributes of a plurality of types from each of the plurality of scanned files in the plurality of formats, wherein the plurality of gleaned attribute types differ for protocols used to receive the plurality of scanned files, and each of the plurality of scanned files are received according to one of the protocols;

storing the file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database;

indexing specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database;

examining one of the plurality of files;

retrieving from the plurality of records in the database a first record associated with the one of the examined plurality of files;

retrieving from the plurality of records in the database a second record associated with a malicious file;

analyzing the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record ;

analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and

determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file.

10. (Cancelled)

11. (Previously Presented) The computer program product of claim 9 further comprising:

program code for gleaning specific types of file attributes from a specific file as a function of a format of the specific file.

12. (Previously Presented) The computer program product of claim 9 wherein the program code for indexing file attributes indexes according to a secure hash of the contents of each specific file.

13. (Previously Presented) The computer program product of claim 9 wherein the program code for indexing file attributes indexes according to a cyclical redundancy check of the contents of each specific file.

14. (Previously Presented) The computer program product of claim 9 further comprising:

program code for receiving a plurality of copies of a selected file of the plurality of files; and

program code for storing each of the plurality of copies as a separate record in the plurality of records, each separate record indexed according to the contents of the selected file of the plurality of files, such that the each separate record can be accessed by a single index.

15. (Original) The computer program product of claim 9 further comprising:

program code for deleting records from the database after the records have been stored for a specific period of time.

16. (Currently Amended) A computer system for gleaning file attributes independently of file format, the computer system having a computer readable storage

medium storing computer-executable instructions, the computer-executable instructions comprising:

a reception module, configured to receive a plurality of files in a plurality of formats;

a scanning module, configured to scan the plurality of received files in the plurality of formats, the scanning module communicatively coupled to the reception module;

a gleaning module, configured to glean file attributes of a plurality of types from each of the plurality of scanned files in the plurality of formats, wherein the plurality of gleaned attribute types differ for protocols used to receive the plurality of scanned files and each of the plurality of scanned files are received according to one of the protocols, the gleaning module communicatively coupled to the scanning module;

a storage module, configured to store file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database, the storage module communicatively coupled to the gleaning module;

an indexing module, configured to index specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database, the indexing module communicatively coupled to the storage module;

an examining module, configured to examine one of the plurality of files, the examining module communicatively coupled to the storage module;

a retrieval module, configured to retrieve from the plurality of records in the database a first record associated with the examined one of the plurality of files, the retrieval module communicatively coupled to the examining module and the storage module;

the retrieval module, also configured to retrieve from the plurality of records in the database a second record associated with a malicious file;

an analysis module, configured to analyze the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record; the analysis module communicatively coupled to the retrieval module;

the analysis module, also configured to analyze one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and

a status module, configured to determine whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file, the status module communicatively coupled to the analysis module.

17. (Cancelled)

18. (Previously Presented) The computer system of claim 16 wherein:

the gleaning module is further configured to glean specific types of file attributes from a specific file as a function of a format of the specific file.

19. (Previously Presented) The computer system of claim 16 wherein the indexing module is further configured to index specific file attributes according to a secure hash of the contents of each specific file.

20. (Previously Presented) The computer system of claim 16 wherein the indexing module is further configured to index specific file attributes according to a cyclical redundancy check of the contents of each specific file.

21. (Previously Presented) The computer system of claim 16 wherein:

the reception module is further configured to receive a plurality of copies of a selected file of the plurality of files; and

the storage module is further configured to store each of the plurality of copies as a separate record in the plurality of records, each separate record indexed according to the contents of the selected file of the plurality of files, such that the each separate record can be accessed by a single index.

22. (Cancelled)

23. (Cancelled)

24. (Previously Presented) The method of claim 1 further comprising:
responsive to determining the status of the examined one of the plurality of files to be malicious, blocking the examined one of the plurality of files.

25. (Previously Presented) The method of claim 1 further comprising:
responsive to determining the status of the examined one of the plurality of files to be legitimate, not blocking the examined one of the plurality of files.

26. (Previously Presented) The method of claim 1 further comprising:
applying at least one rule specifying how to use the gleaned file attributes to process the examined one of the plurality of files.

27. (Previously Presented) The method of claim 26 further comprising:
selecting the at least one rule from a plurality of rules to apply specifying how to use the gleaned file attributes to process the examined one of the plurality of files.

28. (Previously Presented) The method of claim 1, wherein the plurality of files are received from a network connection.